FIRST COMMUNITY BANK
OF MOULTRIE COUNTY
Member F.D.I.C.

9 January 2026 | Issue No. 28

Be cyber smart to stay cyber safe.

Guarding Your ATM and Payment Card

Summary

Payment cards are exceptionally convenient for consumers, and they come in various types –ATM, credit, debit, EBT – that enable low-friction banking and shopping. You probably use more than one. But you may not be aware of the various scams and tools fraudsters use to steal your payment information at the terminal and convert it into a substantial payday. It only takes seconds to install a scam device, and they can be anywhere. Fortunately, it takes even less time to protect your ATM and payment card.

Scam Devices

Scam devices have been found on ATMs, Point of Sale (POS) terminals, gasoline pumps – everywhere people use a card to pay. These devices capture personal data and PINs via video, digital download, or wireless transmission to the scammer. For example:

- **Pinhole cameras** are installed to record PIN entries (**see image example 1**) and are so small they're hard to detect. Note that pinhole cameras may be placed anywhere on or near the machine.
- **Skimmers** installed in the terminal or over its reader (**see image example 2**) steal credit/debit card data from the magnetic stripe or chip.

- **Keylogging** keypads are overlays that cover the real keyboard, used to record a customer's keystrokes (**see image example 3**). If the criminal knows what you type, they know your PIN.

Protecting Your Payment Card

- Inspect ATMs, POS terminals, and other card readers for loose, crooked, damaged, or scratched parts. If you notice something suspicious, use a different terminal.
- Check for keylogging overlays by lifting the edge of the keypad – a gentle tug is all it takes.
- Prevent cameras from recording your PIN by shielding your entry with your hand. Keep in mind that a pinhole camera may be present anywhere on or around the terminal.
- If possible, use ATMs in well-lit, high-traffic locations. Machines are less vulnerable in places where someone might notice a threat actor tampering with them.
- Be especially alert for skimming devices in tourist areas, where card readers are used a lot.
- When possible, use debit and credit cards with chip technology rather than magnetic stripes, which are more vulnerable to theft.
- Avoid using your debit cards for multiple accounts – the compromise of one card gives criminals access to all the accounts. Use a credit card instead.
- Routinely monitor your card accounts to promptly identify any unauthorized transactions. If possible, set up email or text-message alerts to notify you of account transactions.
- Proactively review the account security options. You may be able to set up multifactor authentication or freeze an account between transactions. Such steps may seem inconvenient, but they significantly reduce the risk of financial losses.
- Never give your PIN in response to a call, text, or email. Organizations that have your information would not request your PIN. They use other means to authenticate your account. If you receive a request, look up the source's website and contact them to check your account.
- Always use a strong PIN. Avoid using PINs that may be easily guessed, such as strings of the same or consecutive numbers (e.g., 11111 or 1234).
- Find out if your account will allow you to temporarily block or freeze transactions on the account.

Tips for Paying at the Pump

- Choose the fuel pump closest to the store and in direct view of the attendant. These pumps are less likely to be targets for skimmers.
- Run your debit card as a credit card. If that's not an option, cover the keypad when you enter your PIN. You should also examine the keypad before use for any inconsistencies in coloring, material, or shape. These inconsistencies might suggest that a foreign device (keypad overlay) is present.
- Consider paying inside with the attendant, not outside at the pump.
- Tap the card instead of swiping or inserting it when paying at the pump (if the card and terminal allow for it). Tap-to-pay transactions are more secure and less susceptible to compromise.

What to do if You Are Scammed

- Contact your financial institution immediately if the ATM doesn't return your card after you finish or cancel a transaction. It may indicate a foreign device is in the card reader.
- If you suspect your EBT card was compromised, immediately contact your state benefits agency or card issuer. Promptly change your PIN if any funds remain in your account.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.govand the police.

Getting Help

If you identify suspicious activity involving your financial institution, contact them immediately.

12120 Sunset Hills Rd, Reston
VA 20190